WHITE PAPER

PROTEGGI LE TUE API DURANTE LA PEAK SEASON

Guida completa per l'e-commerce

UNGUESS Security

INTRODUZIONE

Perché la sicurezza delle API è fondamentale durante la Peak Season

Durante il **Black Friday** e le **festività natalizie**, gli e-commerce vedono un enorme aumento del traffico e delle transazioni, rendendo le **API** un **obiettivo primario per i cyber attacchi**. Le **API**, o **Application Programming Interfaces**, sono il cuore delle operazioni digitali, poiché connettono servizi critici e abilitano le funzionalità principali di un sito web o di una piattaforma e-commerce.

Tuttavia, questo espone gli e-commerce a rischi significativi, dato che **le API non protette possono diventare punti di ingresso per attacchi informatici**.

Nel 2023 il

60%

delle **organizzazioni** ha subìto almeno una **violazione** legata alle **API** negli ultimi due anni

Scopri di più

Le violazioni legate alle API includono **perdite di dati**, **danni finanziari** e **compromettono la reputazione aziendale**.

Con questo white paper, esploreremo le **principali minacce alle API** durante la **peak season** e forniremo consigli pratici per proteggerle, garantendo la continuità delle tue operazioni.

LE MINACCE PIÙ COMUNI PER LE API DURANTE IL BLACK FRIDAY

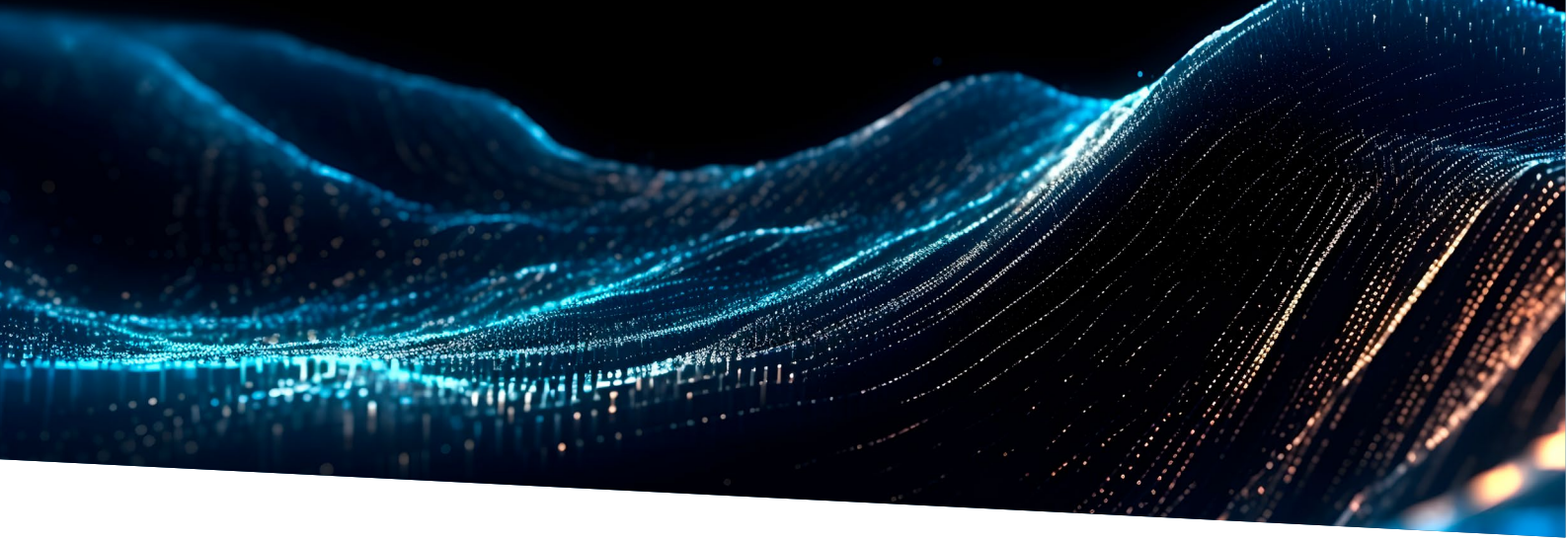
Durante la peak season, gli attacchi informatici diventano più frequenti e sofisticati

DDoS
Gli attacchi DDoS (Distributed Denial of Service) mirano a sovraccaricare le API con richieste massicce, causando downtime o rallentamenti. Questo può portare a perdite di vendite e clienti frustrati.

AUTENTICAZIONE E AUTORIZZAZIONE INSUFFICIENTI
Le aziende devono fornire aggiornamenti regolari sulle misure di sicurezza e report dettagliati su eventuali vulnerabilità.

FURTO DI DATI
Obbligo di informare chiaramente gli utenti su rischi e misure di protezione implementate.

INIEZIONI DI CODICE MALIGNO
Attacchi come SQL Injection e XXS sfruttano le vulnerabilità delle API per inserire codice dannoso, compromettendo la sicurezza dei dati e l'integrità del sistema.



IMPATTO DEGLI ATTACCHI ALLE API

Perdita di dati, reputazione e fatturato

Le violazioni delle API hanno conseguenze significative che vanno oltre la perdita immediata di dati. Il **52% delle organizzazioni** ha riportato **danni finanziari** a seguito di **violazioni delle API**, e molti hanno subito un **calo di fiducia** da parte dei clienti e dei partner commerciali. Tra le conseguenze più comuni troviamo:

PERDITA DI VENDITE DURANTE IL BLACK FRIDAY
Ogni minuto di downtime può costare migliaia di euro in vendite perse, soprattutto durante i momenti di picco delle festività.

DANNO ALLA REPUTAZIONE
Le violazioni legate ai dati sensibili possono compromettere la fiducia dei clienti e portare a una perdita di clienti a lungo termine.

SANZIONI E MULTE LEGALI
In caso di violazione di dati, le aziende possono essere soggette a pesanti multe per il mancato rispetto delle normative sulla protezione dei dati, come il GDPR.

BEST PRACTICES PER PROTEGGERE LE API DURANTE LA PEAK SEASON

Ecco alcune delle migliori strategie per proteggere le tue API durante il periodo delle festività:

Validazione degli Input

Imposta limiti alle richieste che possono essere fatte a una singola API per ridurre il rischio di sovraccarico e prevenire attacchi DDoS.

Crowdtesting delle API

Coinvolgi una rete globale di tester per simulare scenari reali di attacco e identificare vulnerabilità nascoste prima che possano essere sfruttate dagli hacker.
Il crowdtesting ti consente di ottenere una visione completa delle tue vulnerabilità operative.

Rate Limiting

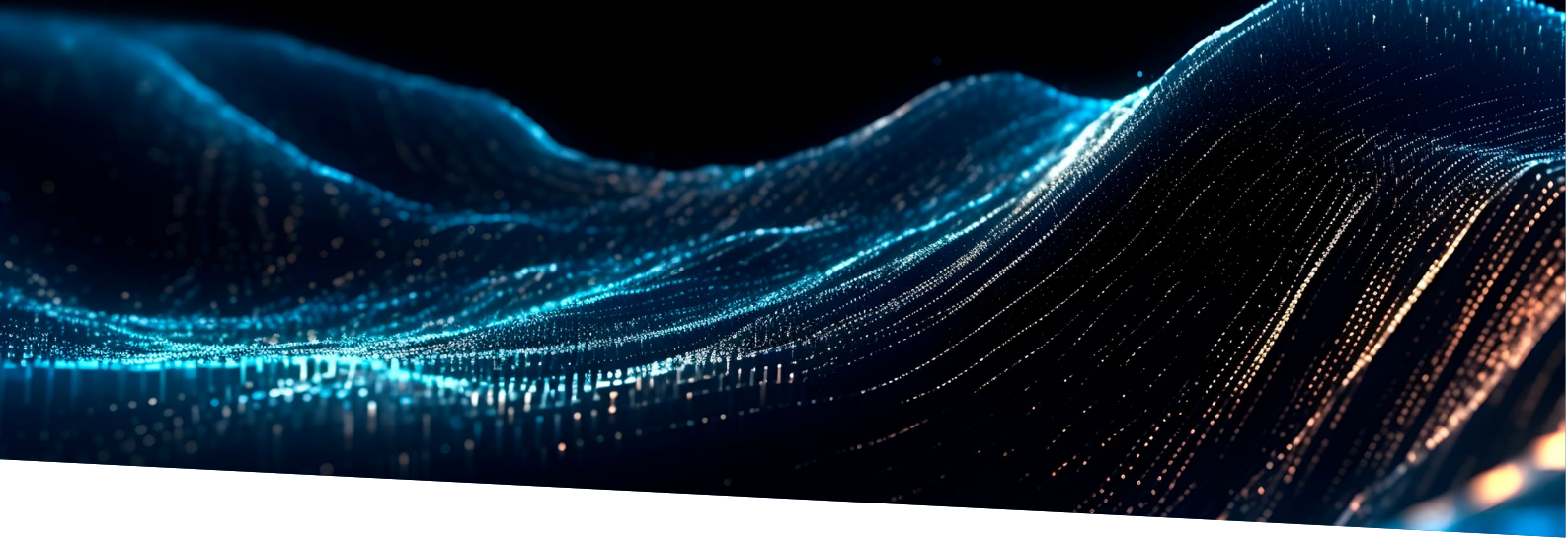
Imposta limiti alle richieste che possono essere fatte a una singola API per ridurre il rischio di sovraccarico e prevenire attacchi DDoS.

Monitoraggio Continuo

Implementa soluzioni di monitoraggio in tempo reale per rilevare anomalie o attacchi in corso. Questo permette di intervenire tempestivamente in caso di minacce.

Autenticazione Forte

Utilizza protocolli di autenticazione avanzati come OAuth e l'autenticazione a due fattori (2FA). Garantisci che solo utenti autorizzati possano accedere alle tue API, proteggendo i dati sensibili.



IL RUOLO DEL CROWDTESTING NELLA SICUREZZA DELLE API

Testa il tuo e-commerce con condizioni reali e trova vulnerabilità nascoste

Il **crowdtesting** è una strategia efficace per **testare la sicurezza** delle API in condizioni reali. In un contesto come il **Black Friday**, dove l'**aumento del traffico** può evidenziare **falle nella sicurezza**, il crowdtesting permette di identificare vulnerabilità nascoste e testare l'efficacia delle difese contro attacchi su larga scala.

SIMULARE ATTACCHI SU LARGA SCALA

Tester distribuiti a livello globale simulano attacchi DDoS, furto di dati, e autenticazioni malevole per verificare la robustezza delle API

IDENTIFICARE VULNERABILITÀ NASCOSTE

Testando le API in condizioni reali, puoi individuare vulnerabilità che potrebbero sfuggire ai test interni tradizionali

PREVENIRE DOWNTIME COSTOSI

Riduci al minimo il rischio di downtime o rallentamenti, garantendo che le tue API funzionino al meglio durante i periodi di picco.

PROTEGGI IL TUO E-COMMERCE E LE TUE API DURANTE IL BLACK FRIDAY

Le **API sono fondamentali** per il successo delle operazioni e-commerce, ma la loro sicurezza non può essere sottovalutata. Con l'**aumento del rischio** durante la **peak season**, è essenziale adottare misure proattive per prevenire attacchi e garantire la continuità delle operazioni.

Scarica ora la nostra guida completa e scopri come UNGUESS può aiutarti a testare e proteggere le tue API in modo efficace!

Non perdere tempo

proteggi le persone ed il tuo business ora!

Scopri UNGUESS Security.

BOOK A DEMO

UNGUESS Security